National Security Agency/
Central Security Service

INFORMATION ASSURANCE CAPABILITIES

ENTERPRISE GRAY IMPLEMENTATION REQUIREMENTS ANNEX V0.8

The guidance given in this Commercial Solutions for Classified (CSfC) Annex, describes how to protect classified data in transit while interconnecting scalable and centrally manageable solutions from Multiple Capability Packages simultaneously across geographically large distances while leveraging existing infrastructure and services.

Version 0.8
12 July 2018

Enterprise Gray Implementation Requirements Annex

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Enterprise Gray (EG) Implementation Requirements Annex	0.8	12 July 2018	• Initial draft of CSfC EG Implementation Requirements Annex. Posted for customer review and comments.

Enterprise Gray Implementation Requirements Annex

Table of Contents

1 Introduction 1

2 Multiple Capability Packages 2

3 Centralized Management 2

3.1 Enterprise Gray Implementation Guide Components 4

3.1.1 Outer Firewall 4

3.1.2 Outer Encryption Component 4

3.1.3 Gray Firewall/Encryption Component 5

3.1.4 Gray Administration Workstation 6

3.1.5 Gray Security Information and Event Management (SIEM) 7

3.1.6 Gray Authentication Server 7

3.1.7 Gray Domain Name System (DNS) 7

3.1.8 Gray Network Time Protocol (NTP) 7

3.2 Gray Certificate Authority (CA) and Revocation Status Services 8

3.3 Certificate Revocation List (CRL) Distribution Point (CDP) & Online Certificate Status Protocol (OCSP) 8

4 Scalibility 9

4.1 Authorized Ports, Protocols, and Internet Protocol Addresses 11

4.1.1 Black Network 11

4.1.2 Gray Network 11

5 Site Survivability 13

6 Requirements Overview 15

6.1 Threshold and Objective Requirements 15

6.2 Requirements Designators 16

6.3 Gray Firewall/Encryption Component (FW) & Additional Requirements (AR) 17

Appendix A. Acronyms 22

Enterprise Gray Implementation Requirements Annex

TABLE OF FIGURES

Figure 1. Multiple CPs Using the Same Components 2
Figure 2. Sites A and B Utilizing Gray Services of Main Site 3
Figure 3. Gray Management and Data Services 6
Figure 4. Dynamic Routing 10
Figure 5. Authorized Protocols on Black 11
Figure 6. Authorized Protocols on Gray 13
Figure 7. Minimum Services Needed for Site Survivability 14

LIST OF TABLES

Table 1. Capability Designators 15
Table 2. Requirements Digraph 16
Table 3. Gray Firewall/Encryption Component IPsec Encryption (Approved Algorithms for Classified) 17
Table 4. Multiple CP Requirements 17
Table 5. Central Management Requirements 19
Table 6. Scalability Requirements 21
Table 7. Site-Survivability Requirements 21

Enterprise Gray Implementation Requirements Annex

INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

1 INTRODUCTION

Information Assurance Capability is delivering the Enterprise Gray (EG) Implementation Requirements to meet the increasing demands for customers desiring to implement Commercial Solution for Classified Solutions with the following characteristics:

- Ability to implement Multiple Capability Packages Simultaneously
- Capable of Central Management
- Readily Scalable
- Enhanced Site-Survivability

The Enterprise Gray (EG) Implementation Requirements Annex introduces guidance that helps customers grow and expand their networks across geographically larger distances while leveraging their existing infrastructure and services to manage that growth. This annex references the CSfC Campus Wireless Area Network (WLAN), Mobile Access (MA), and Multi-Site Connectivity (MSC) Data-in-Transit Capability Packages using approved cryptographic algorithms and National Information Assurance Partnership evaluated components. These algorithms, known as the Commercial National Security Algorithm suite, protect classified data using layers of Commercial-Off-The-Self (COTS) products. The Enterprise Gray Implementation Requirements Annex, Version 0.8 takes lessons learned from proof-of-concept demonstrations built by the National Security Agency (NSA) Information System Security Engineers in a CSfC lab.

EG, similar to the CSfC CPs, defines areas of the solution network in terms of Black, Gray, and Red commensurate to the level of protection applied to the data in each area. Specific guidance for the CPs and these defined areas can be found at https://www.nsa.gov/resources/everyone/csfc/capability-packages/. Customers who want to use this documentation to register two or more interconnecting CSfC Solutions must do so with NSA. Additional information about the CSfC process is available on the CSfC web page www.nsa.gov/ia/programs/csfc_program. Both, the Registration Form and Compliance Checklist are available online at https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml. The Enterprise Gray Implementation Requirements Annex Version 0.8, dated 12 July 2018, has not been approved by the Information Assurance Capability Director and is being released for public comments. Please provide comments on the usability, applicability, and/or shortcomings of this guidance to your NSA Client Advocate and the EG annex maintenance team at Enterprise_Gray_team@nsa.gov. Solutions adhering to this guidance must also comply with the Committee on National Security Systems policies and instructions.

2 MULTIPLE CAPABILITY PACKAGES

The CSfC EG Implementation Requirements Annex provides cost effective techniques to deploy all three Data-in-Transit CPs at the same time using centralized certificate and Virtual Private Network (VPN) management. Selecting equipment with the ability to collapse into components for multi-use, allows customers to deploy multiple CPs simultaneously. An example of this is a customer using the same component for encryption and WLAN controller in unison. In this example, the Outer Encryption component would serve as the WLAN Access System used in the Campus WLAN CP and the Outer VPN Gateway in the Mobile Access CP, provided it is on the CSfC components list to serve both functions. EG is controlled and managed as classified and all the Gray Network components are physically protected at the same level as the Red Network. Each component is described more detail in Section 3.

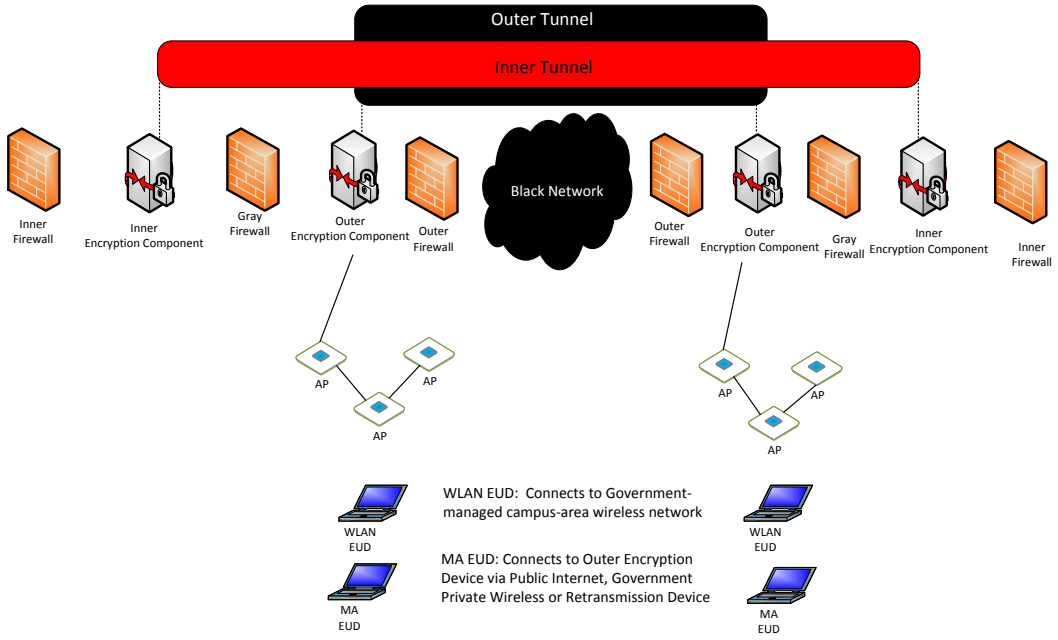

Figure 1. Multiple CPs Using the Same Components

3 CENTRALIZED MANAGEMENT

The administration of components in this annex is key to providing Centralized Gray Management Services. Although Gray Management Services are composed of several components, those described below have specific roles essential to the security of the solution. Each component is accessible only

through the Gray Firewall/Encryption Component and physically protected as classified devices. Interconnecting two or more solutions using Gray Management Services allows flexibility in the placement of some components.

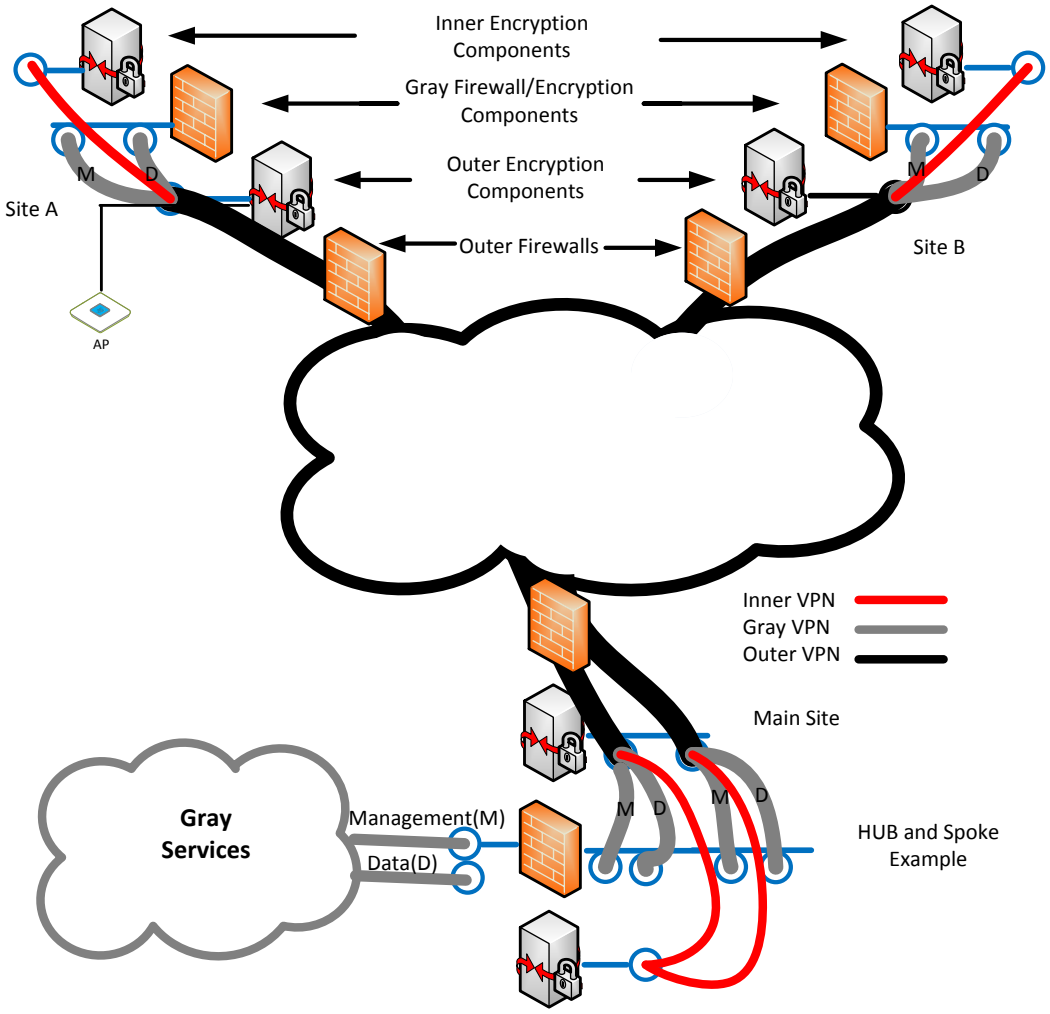

Figure 2. Sites A and B Utilizing Gray Services of Main Site

Generally, the Gray area of a CSfC solution is singly encrypted and under the control of the solution owner, or a trusted third party; however, when extending the Gray services to another site over an untrusted network, two independent layers of encryption must be used to protect management and data. The Gray Firewall/Encryption Component at each site will provide the inner layer of encryption and the Outer Encryption component will provide the Outer layer of encryption to protect Gray

Management traffic between sites. Additionally, both components will use certificates issued by the same Outer Certificate Authority for authentication. The implementing Authorizing Official (AO) may require additional components for encryption separate from the Gray Firewall to reduce risk to the solution.

3.1 Enterprise Gray Implementation Guide Components

3.1.1 Outer Firewall

The Outer Firewall must be incorporated in most CSfC solutions designed to send management and data traffic over an untrusted network. For customers deploying the Multi-Site Connectivity and Campus WLAN CPs, the Outer Firewall is not required. The Outer Firewall is located at the edge of all CSfC solution infrastructures implementing the EG guidance. The external interface of the Outer Firewall only permits Internet Protocol security (IPsec), Internet Key Exchange (IKE) and Encapsulating Security Payload traffic with a destination address of the Outer Encryption component. The internal interface of the Outer Firewall only permits IPsec traffic with a source address of the Outer Encryption component. The Outer Firewall must be physically separated from the Outer Encryption component, as shown in Figure 2.

3.1.2 Outer Encryption Component

The Outer Encryption Component is capable of establishing an encrypted tunnel using IPsec. When used in an EG solution, it can either serve as a peer gateway to other Outer Encryption components of CSfC solutions while providing device authentication, confidentiality, and integrity of data transiting untrusted networks. If the Outer Encryption component is used for Campus WLAN, then it is considered part of the WLAN Access system, which is composed of Access Point(s) and a WLAN Controller capable of initiating and terminating multiple cryptographic tunnels to and from numerous Wireless Clients. For Campus WLAN, it is important to note that depending on the vendor, the Black Gray boundary can either be at the Access Point, or the WLAN Controller. The Outer Encryption component is located between the Outer Firewall and the Gray Firewall. The Outer Encryption component also provides the outer layer of encryption for the protection of Gray and Red services as they traverse the untrusted network. Dynamic Routing is prohibited on the external and internal interfaces of the Outer Encryption component. The component reduces the risk of exposure of information in transit across a Black Network, since the data is placed in a secure tunnel that provides an authenticated and encrypted path between two or more sites.

If the Outer Encryption component is considered a shared outer, then it also has the responsibility of filtering traffic on its Gray Network interface to prohibit Inner Encryption component traffic of different

levels of classification from sending packets between each other since filtering is based on the source and destination address within the packet on the Gray Network.

3.1.3 GRAY FIREWALL/ENCRYPTION COMPONENT

This annex introduces two new functions to CSfC, first time use of dynamic routing in a solution and secondly, a security component serving as a firewall and encryption component at the same time. Dynamic Routing with the use of Virtual Route Forwarding (VRF) is discussed in detail in Section 4.

The Gray Firewall/Encryption Component is located between the Outer and Inner Encryption Components and provides packet filtering for, and access to, Gray Management and Data Services. Additionally, the Gray Firewall/Encryption Component is needed for central management when sharing Gray Services from one site to another site(s) over the untrusted Network. The Gray Firewall/Encryption Component must filter all traffic routed to two or more Inner Encryption Components of different classification. The Gray Firewall/Encryption Component provides the inner layer of encryption for the protection of Gray services as the management and data traffic traversing the Black Network. The Gray Management and data traffic is encrypted using IPsec before being routed through the Outer Encryption component to another site(s) Gray Firewall/Encryption Components as shown in Figure 2. The Outer Certificate Authority (CA) signs the Gray Firewall certificate for IPsec. The Implementing AO may choose to select an additional component from the CSfC components list to serve as Encryption component for Gray Management and data traffic or use a Type 1 Encryption Device.

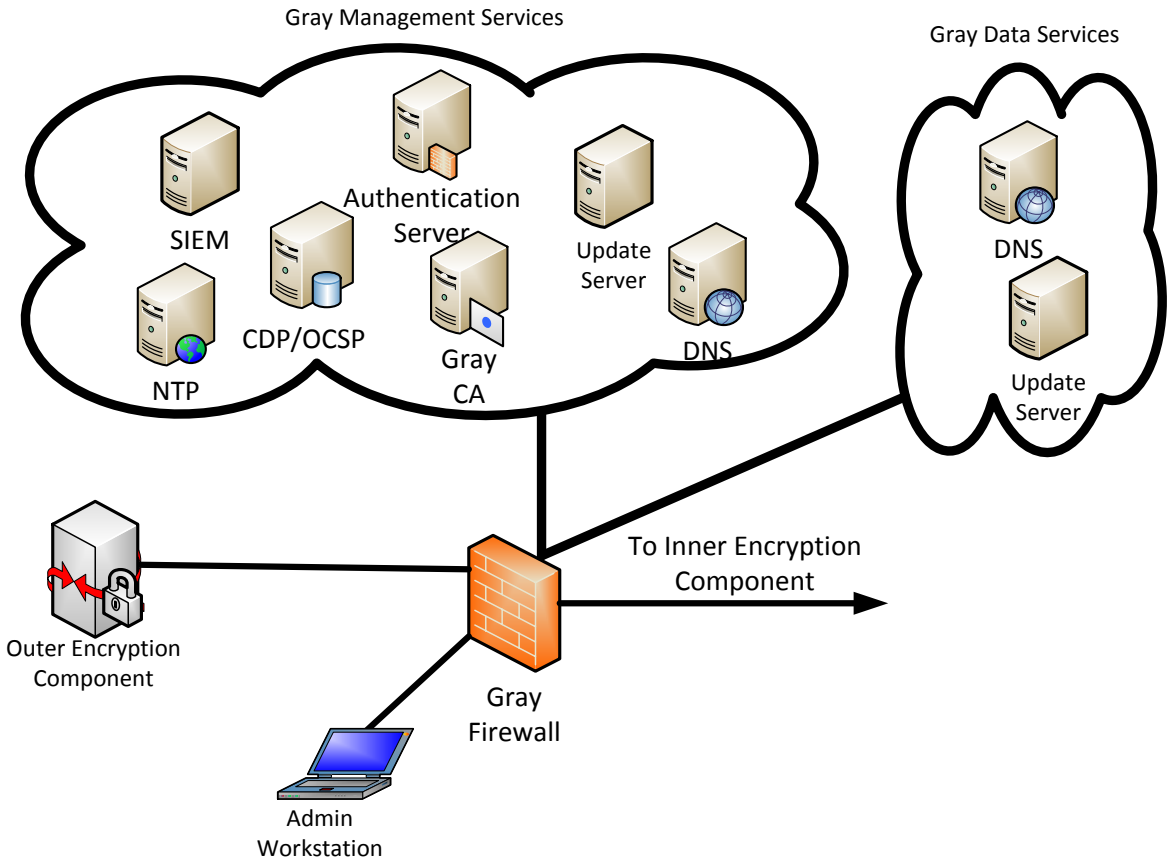

Figure 3. Gray Management and Data Services

3.1.4 GRAY ADMINISTRATION WORKSTATION

The Gray Administration workstation(s) maintains, monitors, and controls all of the security functionality of the Gray Network components across one or more CSfC solutions. This workstation may be used for logging, configuration, and management only. The Gray Administration workstation cannot be used to provision solution components, or an enrollment, or registration authority for a CA. Additionally, the Gray Administration workstation cannot be used to administer the Inner VPN Gateway or Red management services.

3.1.5 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from all Gray components. Log data should be encrypted between the originating components and the Gray SIEM with Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), or IPsec to maintain confidentiality and integrity of the log data.

The EG annex allows customers to deploy multiple CP solutions physically located outside of a secure government facility in tactical environments. Given an increase in accessibility, potential threats cause a need to continuously monitor network traffic and system log data within in the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks against their solution in addition to detecting any configuration errors within infrastructure components. At a minimum, this annex requires alerts, events, and system logs to be sent back to a SIEM at a centralized Operations center to facilitate continuous monitoring of the solution on a daily basis. This minimum review period allows customers in tactical environments to implement solutions in situations where it may not be feasible to perform real-time local monitoring.

3.1.6 GRAY AUTHENTICATION SERVER

The Gray authentication server is required for solutions that support multiple security levels. The authentication server performs mutual authentication with End User Devices (EUDs) using the Outer Encryption component as an Extensible Authentication Protocol pass-through. The Gray authentication server is also required for central management in the administration of Gray Services between the Management Site and Remote Site(s), as shown in Figure 3.

3.1.7 GRAY DOMAIN NAME SYSTEM (DNS)

The Domain Name System is a control plane service responsible for name resolution to Internet Protocol addresses within the Gray Network for both management and data. The Gray management DNS servers can be connected to each other in a hierarchical structure with the main site having the root authoritative DNS which update updates the rest of the DNS servers within the EG network. Domain Name System Security (DNSSEC) is recommended for these DNS servers to ensure the integrity of the responses. Another reason to use DNSSEC is to ensure that the DNS request is not changed or forged.

The Data DNS is required to do Name Resolution for both EUDs and site-to-site connection to ensure the correct Inner Encryption component is connected. The Gray Data DNS server cannot communicate with any other DNS servers and it must be an authoritative DNS.

3.1.8 GRAY NETWORK TIME PROTOCOL (NTP)

Gray Network Time Protocol is responsible for all time synchronization, which is important for time stamps used for certificates and logging within the Gray Network. NTP uses a hierarchical ranking of

time sources for synchronization called strata. For example, stratum zero (0) are high-precision time sources such as atomic clocks. Stratum one (1) are computers that have been synchronized within microseconds to a directly connected stratum 0 time source. Stratum two (2) are computers synchronized and directly connected to a stratum 1 time source, and so on.

3.2 Gray Certificate Authority (CA) and Revocation Status Services

The CA for Outer and Gray Encryption components can be located on a Gray Management network, connected to the Encryption components or offline on the Red network. A Certificate Policy and Certification Practice Statement document must be created or tailored for each CA used in the solution. It is then the AO's responsibility to approve the use of a CAs. If an Outer tunnel CA is an Enterprise CA already running on the necessary Gray Management network, then no additional approval is necessary. It is important to note that no single CA can provide keys to both Inner and Outer Encryption components. Since the Gray Encryption component that creates the inner tunnel for Gray services across an untrusted network resides on the Gray network, it can be signed by the Gray CA.

Each Encryption Component has at least one CA signing certificate (sometimes referred to as a Trust Anchor), it is used by the Encryption Component to authenticate Clients and other Encryption Components within the solution. When centralized management is used, each Encryption Component will have only one CA signing certificate. Otherwise, one CA signing certificate is installed in each Inner Encryption Component for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate will be installed in each Outer Encryption Component for each Outer Tunnel CA used in the system.

3.3 Certificate Revocation List (CRL) Distribution Point (CDP) & Online Certificate Status Protocol (OCSP)

A Certificate Revocation List (CRL) Distribution Point (CDP) is a webserver that hosts CRL files for Encryption Components to check the revocation status of EUDs before allowing a connection to the network. A solution may use CDPs to provide CRLs to Encryption Components before those Encryption Components have established any VPN tunnels. CDPs work when they are placed on the network reachable from the Encryption Component's internal interface: on the Gray Network for Outer Encryption Component and on the Red Network for the Inner Encryption Component(s).

The Online Certificate Status Protocol (OCSP) allows applications to determine the revocation state of a certificate. OCSP is more efficient than CRLs because it automates the certificate revocation status checking. The OCSP client sends a status request to the OCSP responder and will not accept the certificate from the responder until the responder provides an acceptable response. An acceptable

response is the accurate data exchanged between the application checking the status of the certificate and the server providing the status.

4 SCALIBILITY

Given the ability to scale to multiple centrally managed sites and use Dynamic Routing, allows customers more flexibility with continuity of operations. This annex introduces Dynamic Routing for the first time in a CSfC solution. Instead of using the Gray Firewall for dynamic routing, the AO may choose to use an additional component to serve as a Gray Inner encryption component. Dynamic Routing will only be used on the Gray Firewall/Encryption Component to propagate routing information through the Gray Firewall/Encryption Component to share Gray Management and Gray Data services at multiple sites. If dynamic protocols are used, then authentication must be accomplished between solutions Gray Firewall/Encryption Components at all sites.

The following Dynamic Routing protocols are authorized at the Gray Firewall/Encryption Component to support the Enterprise Gray VPN's: Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Intermediate System-Intermediate System (IS-IS), and Border Gateway Protocol (BGP). Additionally, when using Dynamic Routing Protocols, data and management traffic must be separated using Virtual Routing and Forwarding (VRF). Each interface will be assigned to a VRF that is specifically allowed to interact with its respective network plane (Data Plane or Management Plane).

In some cases the implementer may need to import or export routes to establish a VPN tunnel on an interface outside of its respective VRF. The Data and Management VRF would send Internet Key Exchange and Internet Protocol security (IKE/IPsec) traffic to the Outer Encryption Component to travel over its encrypted tunnel. Figure 4 below shows VPN-Untrust that interacts with the Outer Encryption Component. A route on this VRF exists to go to the Gray Firewall/ Encryption Component boundary. This route must be imported from VPN-Untrust into the VPN Gray Data and VPN Gray Management so the Gray Encryption Component knows where to send its IKE/IPsec traffic.

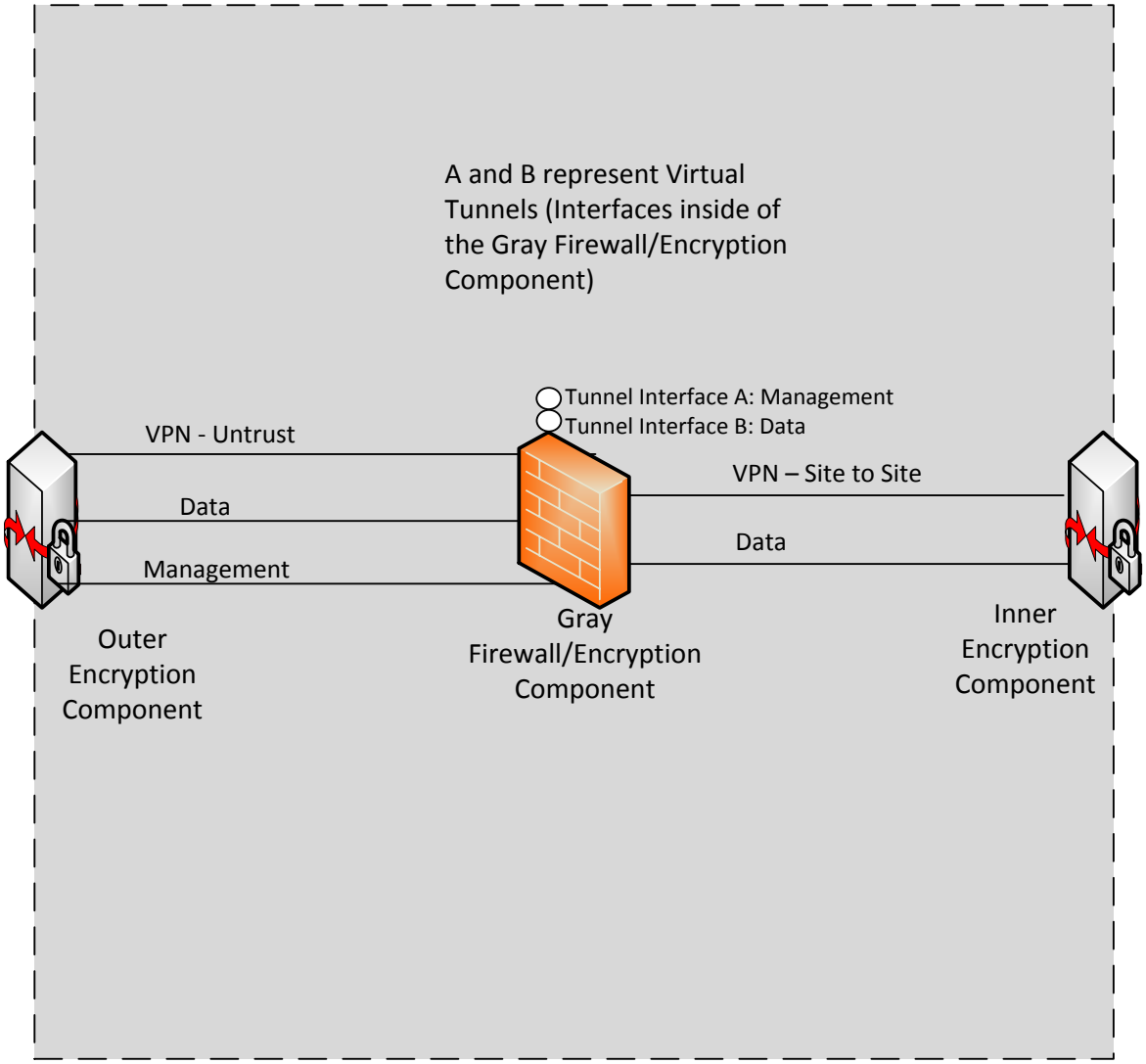

Figure 4. Dynamic Routing

4.1 AUTHORIZED PORTS, PROTOCOLS, AND INTERNET PROTOCOL ADDRESSES

4.1.1 BLACK NETWORK

IKE and IPsec are the only protocols authorized for bi-directional traffic flows between the Outer Encryption Component and the Outer Firewall as shown in Figure 5. A default route may be used at the Outer Firewall and the Outer Encryption Component for egress traffic to the Internet. Hypertext Transfer Protocol Secure (HTTPS) is not authorized for profile download on the Black Network.

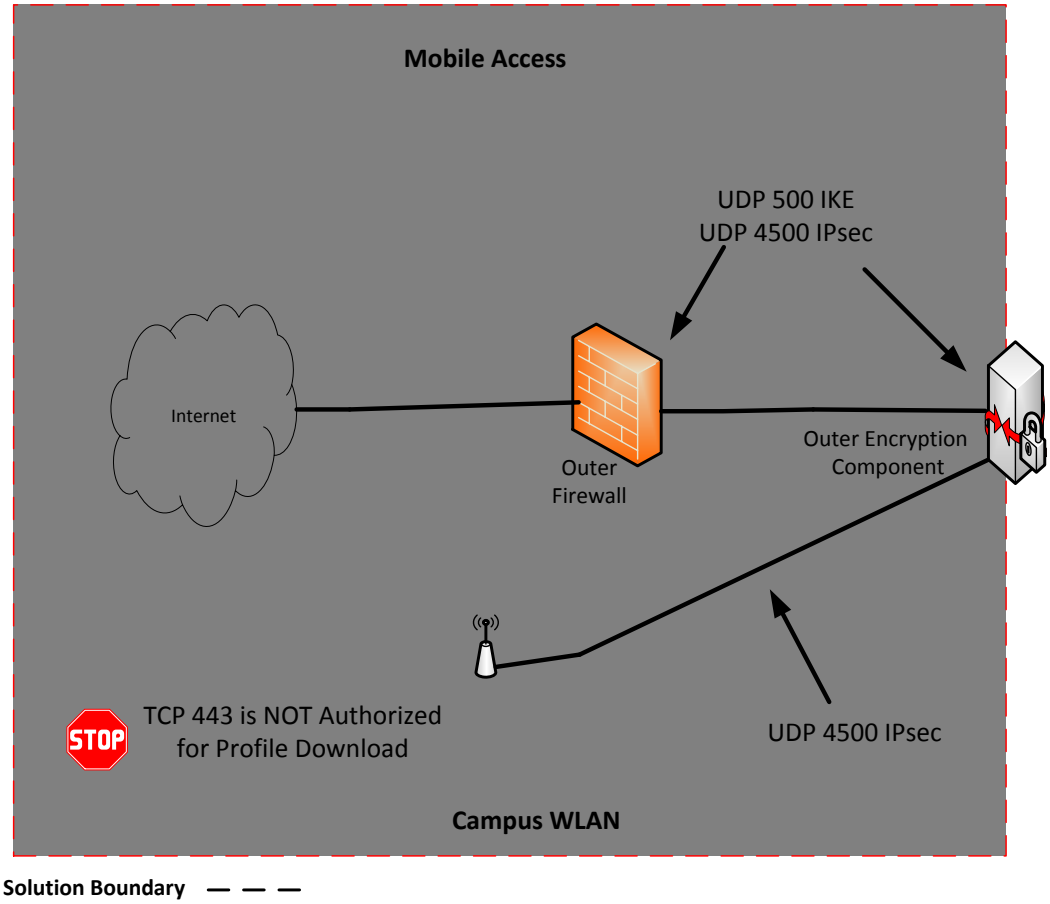

Figure 5. Authorized Protocols on Black

4.1.2 GRAY NETWORK

Between the Outer Encryption Component and the Gray Firewall/Encryption Component, traffic is physically separated into management, data, and VPN as shown in Figure 6. Authorized Management

traffic is Hypertext Transfer Protocol (HTTP), HTTPS, DNS, SSH, radius for authentication, radius for accounting and update services. Management traffic is designed to control networking and server services. **(Mobile Access and Campus WLAN only)** Authorized Data traffic is DNS, IKE, IPsec, and update services. The Outer Encryption Component and Gray Firewall/Encryption Component can only receive Data traffic for the purpose of domain name resolution and security updates, then traverse to any Inner Encryption Component of the same classification level. Authorized VPN traffic is IKE and IPsec and it traverses to the Gray Firewall/Encryption Component to provide Gray VPN services and to Inner VPN Gateways that support Multi-Site Connectivity**.** From the Gray Firewall/Encryption Component to the Inner Encryption Component, traffic is separated into Data and VPN as shown in Figure 6. On the data line, traffic is IKE and IPsec, which only MA and Campus WLAN users may connect. On the VPN line, IKE and IPsec is the only authorized traffic to support MSC users.

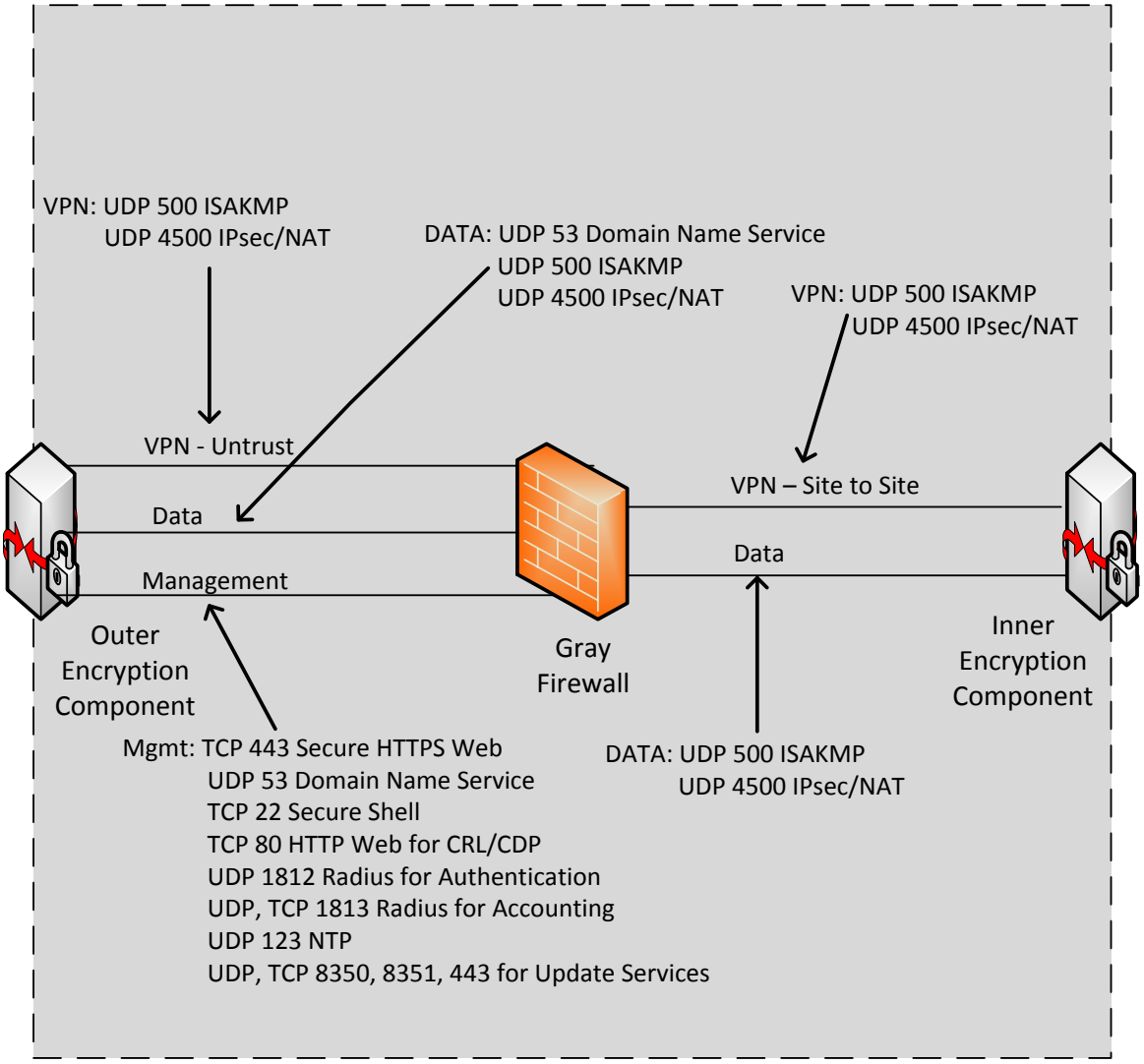

Figure 6. Authorized Protocols on Gray

5 SITE SURVIVABILITY

AOs implementing Enterprise Gray solution guidance may deem site survivability optional for some remote sites depending on the mission of the organization. If site survivability is not a requirement and there is a loss in connectivity, then the remote site will fail closed. In the event of loss connectivity, MA, Campus WLAN, and MSC solutions will not be able to access classified resources.

If the implementing organization requires site survivability, then redundancy equipment is required for remote sites to maintain connectivity, thereby ensuring access to classified resources. Should a loss of connectivity to the centrally managed site occur, then access to resources will be impacted. However, to survive such an event, the remote site will require resources to authenticate users, provide name resolution, certificate revocation list lookups, time synchronization, and centralized log collection.

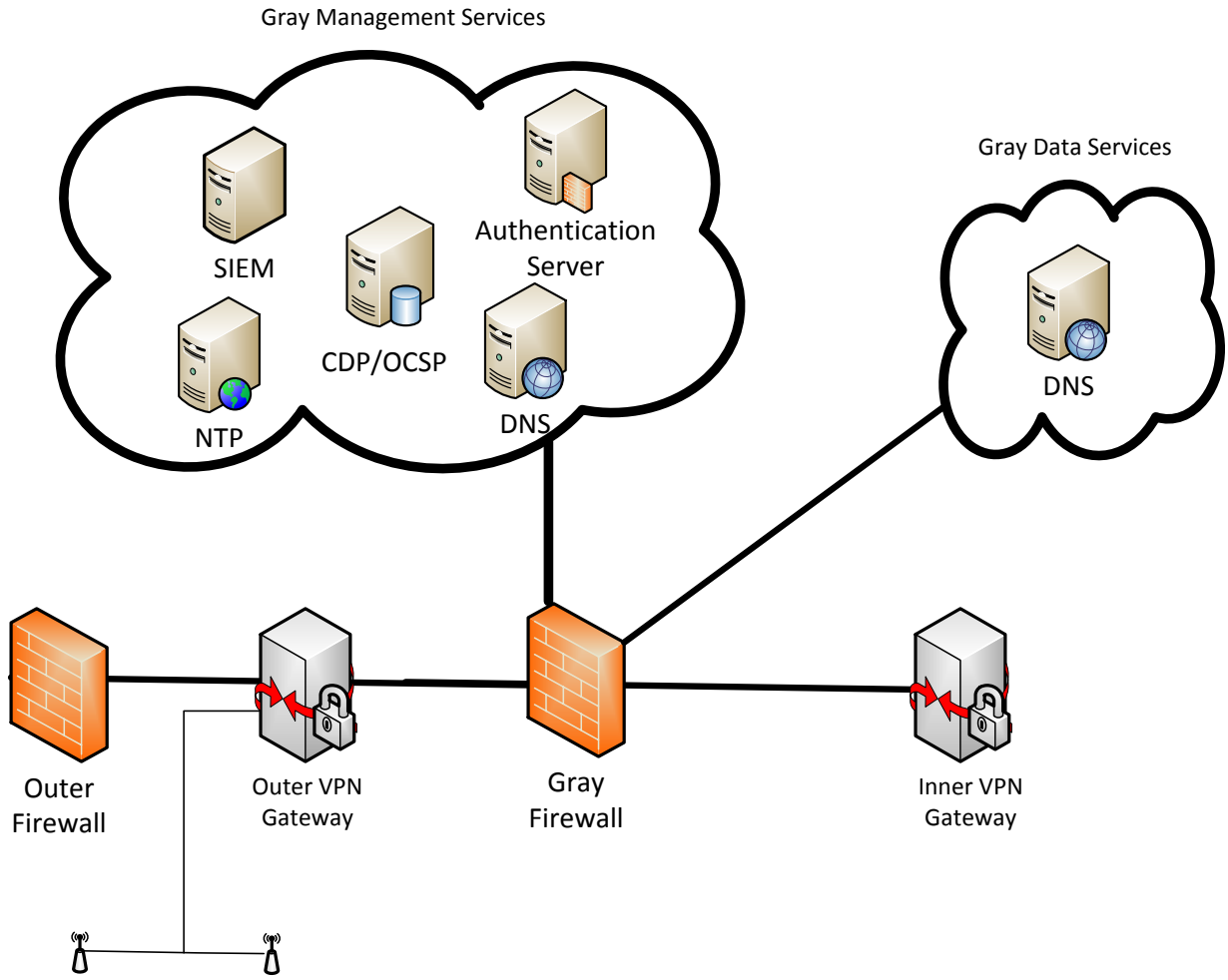

Figure 7. Minimum Services Needed for Site Survivability

6 REQUIREMENTS OVERVIEW

The following three paragraphs (Paragraphs 6.1 through 6.3) specify requirements necessary for the implementation of an Enterprise Gray solution compliant with this Annex. Interconnecting CSfC solutions will follow the requirements of their respective CP.

Guidance provided in this document allows solution owners the flexibility to implement a variety of designs for interconnecting two or more CPs that share a common Gray Network. Although most requirements apply to all CSfC solutions, some requirements only apply to implementations whose high-level designs implement certain features.

Table 1. Capability Designators

Capability Package	Designator	Description
Multiple CPs	All	Requirements pertinent to all Capability Packages. This CSfC Annex comprises all 3 data-in-transit CPs describing how to protect classified data in transit while interconnecting scalable and centrally manageable solutions simultaneously across geographically large distances while leveraging existing infrastructure and services.
Mobile Access	MA	Requirements pertinent to the Mobile Access CP only. This CSfC CP describes how to protect classified data (including Voice and Video) in MA solutions transiting Private Cellular Networks and Government Private Wi-Fi networks
Multi-Site Connectivity	MSC	Requirements pertinent to the MSC CP only. This CSfC CP describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with IPsec.
Campus WLAN	WLAN	Requirements pertinent to the Campus WLAN CP only. This CSfC CP describes how to protect classified data (including Voice and Video) in a WLAN solution transiting Government Private Wi-Fi networks.

6.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist within this documentation. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

When separate Threshold and Objective versions of a requirement exist, the Objective requirement provides more security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not a feasible solution, owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional" in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold/Objective" column indicates that the Threshold equals the Objective (T=O).

Requirements that are listed as Objective in this document may become Threshold requirements in future guidance. Solution owners are encouraged to implement Objective requirements where possible to facilitate compliance with future guidance.

6.2 Requirements Designators

Each requirement in this document is identified by a label consisting of the prefix "EG" a two-letter category, and a sequence number (e.g., EG-FW-7). The Gray Firewall/Encryption Component and General Requirements will be listed together in Tables 4-7. Each table represents a pillar of the Enterprise Gray Implementation Requirements annex.

Table 2. Requirements Digraph

Digraph	Description	Paragraph	Table
FW	Gray Firewall/Encryption Components Requirements	6.3	Tables 4-7
AR	Additional Requirements	6.3	Tables 4-7

6.3 GRAY FIREWALL/ENCRYPTION COMPONENT (FW) & ADDITIONAL REQUIREMENTS (AR)

Table 3. Gray Firewall/Encryption Component IPsec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 6379 IETF RFC 6380
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 IETF RFC 4754 IETF RFC 6380 IETF RFC 7427
Key Exchange/Establishment	ECDH over the curve P-384 Diffie Hellman (DH) Group 20 or DH 3072	NIST SP 800-56A IETF RFC 3526 IETF RFC 5903 IETF RFC 6379 IETF RFC 6380 IETF RFC 7296
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6379 IETF RFC 6380

Table 4. Multiple CP Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-1	The Gray Firewall/Encryption Component and the Outer Encryption Component must use different cryptographic libraries.	T=O		MA/MSC
EG-FW-2	The Gray Firewall/Encryption Component at each site will provide the inner layer of encryption and the Outer Encryption Component will provide the Outer layer of encryption to protect Gray Management traffic between sites.	T=O		ALL
EG-FW-3	The Gray Firewall/Encryption Component must only accept management traffic on the physical ports connected to the Gray	T=O		MSC

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	Management network.			
EG-FW-4	The Gray Firewall/Encryption Component must only permit packets whose source and destination IP addresses match the external interfaces of the Encryption Components supporting the Red Network of the same classification level.	T=O		ALL
EG-FW-5	The Gray Firewall/Encryption Component must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O		ALL
EG-FW-6	The Gray Firewall/Encryption Component must deny all traffic that is not explicitly allowed.	T=O		ALL
EG-FW-7	The Gray Firewall/Encryption Component must filter all traffic routed to two or more Inner VPN Gateways of different classification.	T=O		
EG-FW-8	Remote administration the Gray Firewall/Encryption Component is authorized only using SSHv2, IPsec, or TLS with the appropriate Commercial National Security Algorithm (CNSA) suite for the highest classification of the solution.	T=O		ALL
EG-FW-9	The Gray Firewall/Encryption Component must not permit split-tunneling.	T=O		ALL
EG-AR-01	An Outer Firewall is required between the Outer Encryption Component and the Black Network.	T=O		MA/MSC
EG-AR-02	The Black Firewall must not have a physical connection to the Gray Management Network	T=O		MA/MSC
EG-AR-03	EUDs provisioned for a Mobile Access solution must be used solely for a MA solution and not used to access any resources other than the Red Network it communicates via two layers of encryption.	T=O		MA
EG-AR-04	EUDs provisioned for a Campus WLAN solution	T=O		WLAN

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	must be used solely for a WLAN solution and not used to access any resources other than the Red Network it communicates via two layers of encryption.			

Table 5. Central Management Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-10	The Gray Firewall/Encryption Component must use Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (e.g., GRE)	T=O		ALL
EG-FW-11	The packet size for packets leaving the external interface of the Gray Firewall/Encryption Component must be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for Ipv4) or Path MTU (PMTU) (for Ipv6) and should consider the Outer VPN Gateway MTU/PMTU values for achievement.	O	NONE	ALL
EG-FW-12	The Gray Firewall/Encryption Component must permit IKE and IPsec traffic between End User Device Clients and Encryption Components protecting networks of the same classification level.	T=O		MA WLAN
EG-FW-13	The Gray Firewall/Encryption Component must allow HTTP traffic between the Authentication Server and the Gray CDP or OCSP responder.	T	EG-FW-14 AND EG-FW-5	ALL
EG-FW-14	The Gray Firewall/Encryption Component must allow HTTP GET request from the Authentication Server to the Gray CDP or OCSP responder for the URL of the CRL OCSP Response needed by the Encryption Component and block all other HTTP request.	O	EG-FW-13	ALL

Enterprise Gray Implementation Requirements Annex

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-15	The Gray Firewall/Encryption Component must allow HTTP responses from the Gray CDP or OCSP responder to the Authentication Server that contains a well-formed CRL per IETF RFC 5280 or OCSP Response per RFC 6960 and block all other HTTP responses.	O	EG-FW-13	ALL
EG-FW-16	The Gray Firewall/Encryption Component must only accept management traffic on the physical ports connected to the Gray Management network.	T=O		ALL
EG-FW-17	The Gray Firewall/Encryption Component must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O		ALL
EG-FW-18	The Gray Firewall/Encryption Component must deny all traffic that is not explicitly allowed.	T=O		ALL
EG-FW-19	The Gray Firewall must allow control plane traffic (e.g., NTP, DHCP, and DNS).	T=O		ALL
EG-FW-20	A Gray Firewall must only be administered from a workstation designated for managing Gray components only.	T=O		ALL
EG-FW-21	Remote administration the Gray Firewall is authorized only using SSHv2, IPsec, or TLS with the appropriate CNSA suite for the highest classification of the solution.	T=O		ALL
EG-AR-05	Accessibility to all components composing the Gray Management Services must be accessible only through the Gray Firewall/Encryption Component.	T=O		ALL
EG-AR-06	Two independent layers of encryption must be used when extending Gray Services to other site(s) over an untrusted network.	T=O		ALL

Table 6. Scalability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-07	If Dynamic Routing Protocols are used, then Dynamic Routing Protocols must authenticate to accept routing information Gray Firewalls.	T=O		ALL
EG-AR-08	If Dynamic Routing Protocols are used, then those routes must use Virtual Routing and Forwarding (VRF) to separate Data and Management traffic.	T=O		ALL
EG-AR-09	If Dynamic Routing Protocols are used, then implementers must use one of the following: RIP, OSPF, EIGRP, BGP, and IS-IS.	T=O		ALL

Table 7. Site-Survivability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-10	For site survivability, implementers must use a RADIUS server for the authentication of EUDs and Encryption Components should a loss of connection to the main site occur.	T=O		ALL
EG-AR-11	For site survivability, implementers must use a Gray Data DNS on the site(s) that mirror the DNS on the main site. This allows for EUDs and site-to-site interfaces to connect to the proper Inner Encryption Component.	T=O		ALL

APPENDIX A. ACRONYMS

Acronym	Definition
AO	Authorizing Official
BGP	Border Gateway Protocol
CA	Certificate Authority
CDP	Certificate Revocation List (CRL) Distribution Point
COTS	Commercial-Off-the-Shelf
CP	Capability Package
CNSA	Commercial National Security Algorithm
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
DNS	Domain Name System
DNSSEC	Domain Name System Security
EG	Enterprise Gray
EIGRP	Enhanced Interior Gateway Routing Protocol
FW	Firewall
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IS-IS	Intermediate System-Intermediate System
MA	Mobile Access
MTU	Maximum Transmission Unit
NSA	National Security Agency
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSPF	Open Shortest Path First
PMTU	Path Maximum Transmission Unit
RIP	Routing Information Protocol
SIEM	Security Information & Event Management
SSH	Secure Shell
SSHv2	Secure Shell version 2
TLS	Transport Layer Security
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WLAN	Wireless Local Area Network